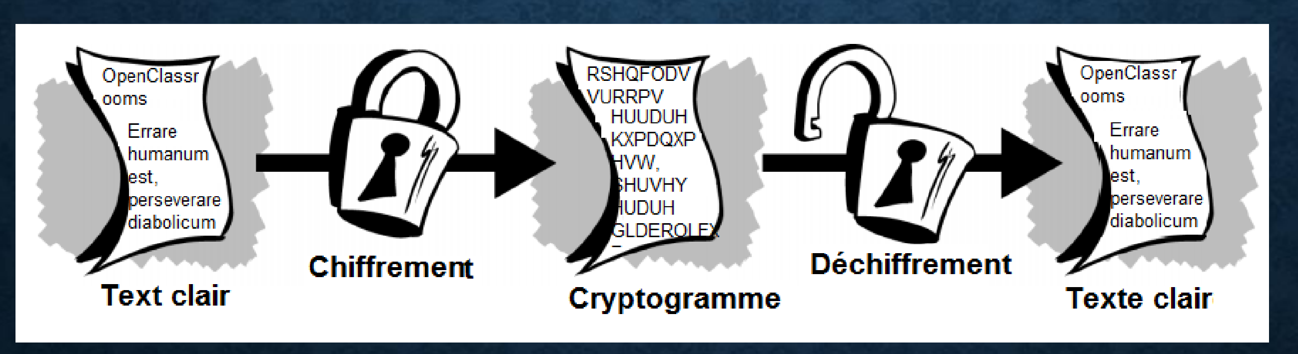
LE CHIFFREMENT DES DONNÉES (CRYPTAGE)



1- POURQUOI CHIFFRER LES DONNÉES

- Chiffrer (crypter) les données (messages, images, etc.), consiste à les rendre illisibles. Il est utilisé pour protéger les données et se repose sur l'ensemble des techniques que l'on appelle **techniques de cryptographie**.

- Donc, le chiffrement est l'opération qui consiste à transformer une donnée (dite "claire") en une donnée qui ne peut être lue que par son créateur et son destinataire (donnée dite "chiffrée" ou "cryptée").



- L'opération qui permet de récupérer la donnée claire à partir de la donnée chiffrée s'appelle le déchiffrement (décryptage).

2- HISTORIQUE DU CHIFFREMENT

- Le chiffrement ne date pas d'aujourd'hui, il remonte à la civilisation babylonienne environ 300 ans avant notre ère.

- Plusieurs méthodes de chiffrement ont vu le jour (l'Atbsh des Hébreux (-500), la scytale à Sparte (-400), le carré de Polybe (-125), …), et la plus célèbre que l'histoire retiendra est le **chiffre de Jules César**.

- Ce dernier ne faisait pas confiance à ses messagers lorsqu'il devait envoyer des messages à ses généraux. Il décida donc de remplacer les lettres A dans ses messages par des lettres D, les B par des E et ainsi de suite.

- Cette méthode est une méthode dite de "chiffrement par substitution simple".

- Voir l'exemple à la page suivante →

HISTORIQUE DU CHIFFREMENT - CHIFFRE DE JULES CÉSAR

- **La clé** pour ce type de chiffrement était le **décalage à 3** dans l'alphabet:

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

Exemple

Texte clair :

errare humanum est, perseverare diabolicum

Texte chiffré :

HUUDUH KXPDQXP HVW, SHUVHYHUDUH GLDEROLFXP

BREF HISTORIQUE DU CHIFFREMENT – ENIGMA

- À l'avènement de la Première Guerre Mondiale, les procédés de chiffrement/déchiffrement se sont accélérés.

- Les Allemands ont mis en place un système à **crypter/décrypter** appelée **Enigma,** en 1918, afin de communiquer entre leurs différentes forces militaires.

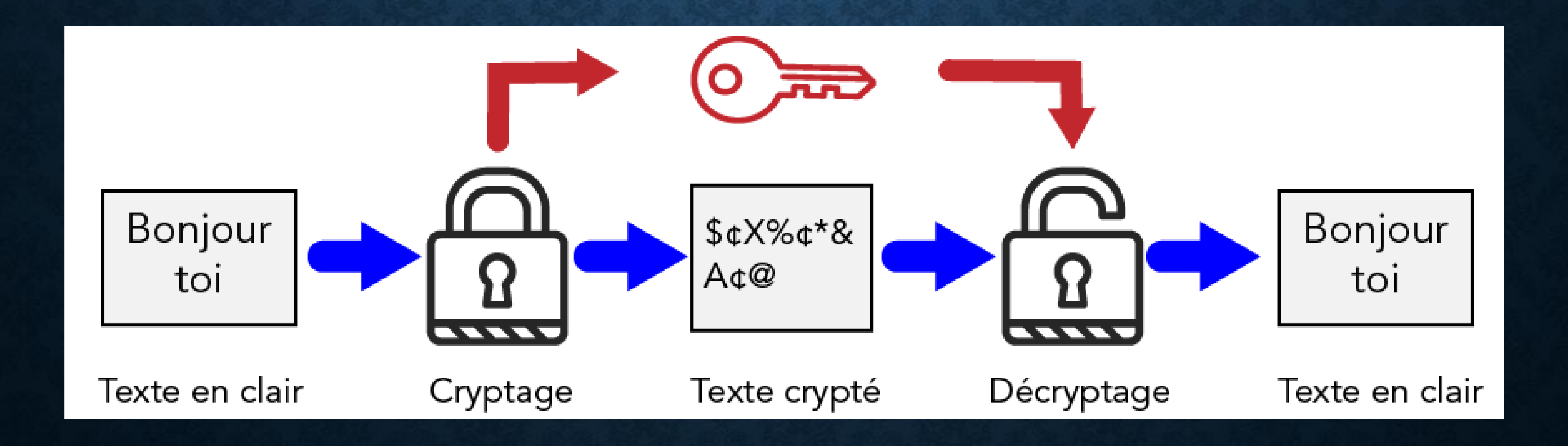
- Pour percer **le code d'Enigma**, les Polonais ont inventé une machine appelée "Bombe", mais c'est Alan Turing qui découvrit le système de code d'Enigma en 1944 (et qui posa à l'occasion les bases du premier ordinateur !).



BREF HISTORIQUE DU CHIFFREMENT – CHIFFREMENT À CLÉ SECRÈTE

- Aujourd'hui, à l'ère où l'usage des ordinateurs et d'Internet est devenu quotidien, le **chiffrement et le déchiffrement (cryptage/décryptage)** sont passés de machines mécaniques, comme Enigma, à des procédés numériques **(logiciels).**

- La méthode de chiffrement la plus utilisée est le **chiffrement avec des clés secrètes.**



3- FONCTIONNEMENT DU CHIFFREMENT AVEC DES CLÉS
CHIFFREMENT SYMÉTRIQUE

- Le premier type de chiffrement est le **chiffrement symétrique.**
- Cette méthode se repose sur **une seule clé secrète** pour chiffrer et déchiffrer les données.
- C'est à dire qu'une même clé permet de chiffrer et de déchiffrer le contenu des données.
- Les systèmes symétriques **sont très rapides**, pour chiffrer un gros volume d'information.
- C'est un mécanisme difficile à briser lorsqu'on utilise **une grande clé**.



3.1- FONCTIONNEMENT DU CHIFFREMENT SYMÉTRIQUE

Comment crypter un fichier en utilisant le cryptage symétrique?

- Installez un logiciel de cryptage symétrique, comme (**BitLocker** de Windows 10, **FileVault** du MAC, **Veracrypt** et **AxCrypt**, …).
- Exécutez le logiciel et choisir le fichier ou dossier à crypté.
- Tapez une **passphrase** (phrase secrète) d'un longueur minimum de 20 caractères et qui sera utilisée par le logiciel de cryptage pour générer **une clé aléatoire secrète**.

Exemple d'une clé:

```
nMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAmuxkTX9+2pGLCh7ugUPV\r
\nqIvu1QXcbLYdDkDgtdLYB4J9MUZ2M1linHAxnxetSzga8lt5GbmBGswee5pFSdCl\r
```

- Un **algorithme de cryptage**, ex. **AES-256**, utilisera cette clé secrète **pour crypter le fichier.**
- Un **algorithme de hachage**, ex. **SHA-512**, sera utilisé pour calculer **une signature** (empreinte digitale) pour s'assurer que les données ne sont pas modifiés.









3.1.1- ALGORITHME DE CRYPTAGE - AES

- **AES (Advanced Encryption Standard)** est **un algorithme** utilisé pour chiffrer les données.
- Il est implémenté dans des logiciels et du matériel à travers le monde pour chiffrer les données sensibles.
- Le fonctionnement d'**AES** est compliqué mais ce qu'il faut retenir c'est que c'est un algorithme de **chiffrement par bloc**. C'est à dire que les données à chiffrer vont être découpées par blocs.
  - Il utilise **une taille de clé** de **128, 192 ou 256 bits** : **AES-128**, **AES-192** **ou** **AES-256**.
- En effet, les applications telles que WhatsApp, Signal, VeraCrypt ou 7-zip et WinZip utilisent AES pour chiffrer (crypter) les communications ou le contenu.

https://www.mathworks.com/matlabcentral/fileexchange/73412-advanced-encryption-standard-aes-128-192-256

3.1.2- ALGORITHME DE HACHAGE - SHA

- **SHA-256** ou **SHA -512 (Secure Hash Algorithm)**, est un algorithme **de hachage** mise en place par la National Security Agency des États-Unis.

Une fois que le fichier est crypté:

- **SHA-512** va prendre le texte du phrase secrète et le "mouliner" (faire un calcul) pour obtenir **une signature** ("empreinte").
- Exemple: La signature du mot « abcdef » sera « e80b5017098950fc58aad83c8c14978e ».
- Cette signature sera enregistré dans le fichier crypté.

Avant de décrypter le fichier:

- Le logiciel de cryptage va utiliser l'algorithme de hachage pour faire le même calcul et créer une nouvelle signature.
- Il va vérifier si la nouvelle signature est bien la même que la signature enregistré dans le fichier.
- Si elles sont identiques, **donc les données du fichier n'était jamais modifiés.**

3.1.2- ALGORITHME DE HACHAGE - SHA

- **Exemple d’un fichier crypté:**

Secret_Data-txt - Bloc-notes

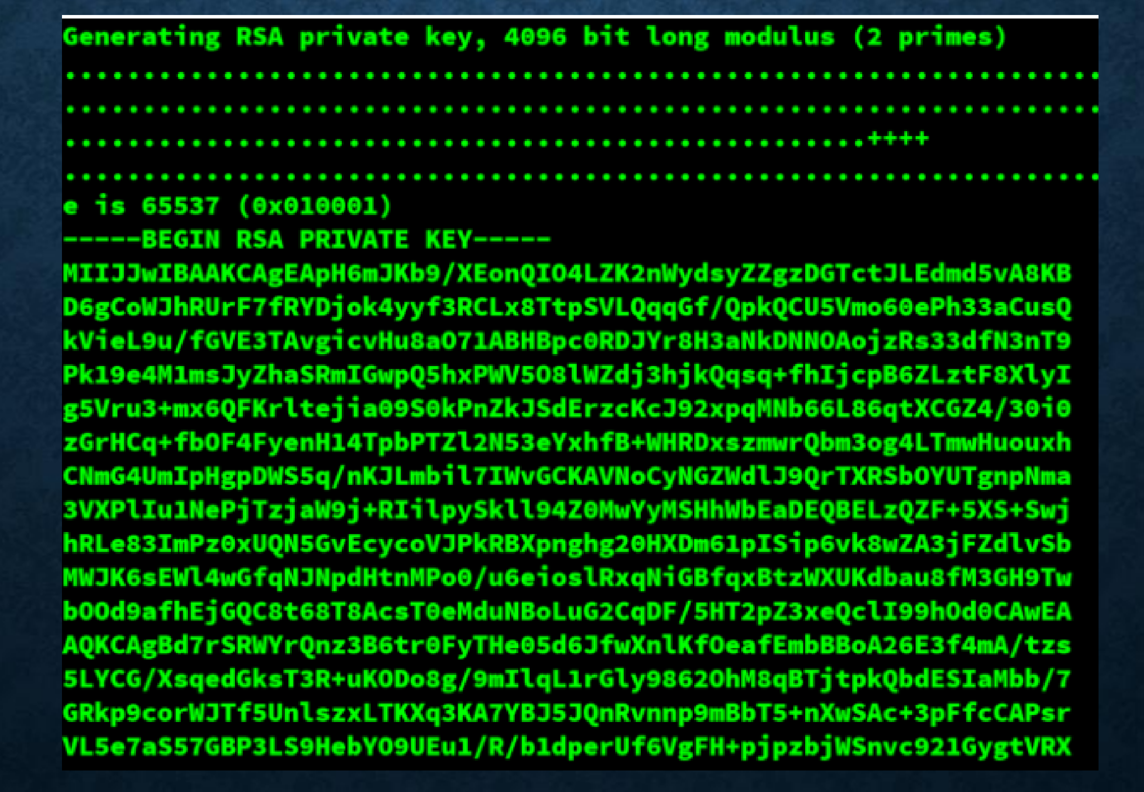
Fichier Edition Format Affichage Aide

À¹.O“ñF y,¡Ùè!
ý
´zé§…(frA¼gÞr¦6,äz„Ò{ÝC«Î
„o»øeZ^ImñÏ¡…P0áÂåµHo éï§Š ¥»–-þ¤uÛ?Zê’ª¡,Oe94sÖALœªlào|‡à£u˜¨ê•bÓ2dÏ
¤òÐKú¥6Ôø'ÃÔšE¼Ä®m\}d5ÌÏab›ÃÊA†9-{€7œtåôfNX)—™žL¦ùÙ`Æ´<ä’žø(‰½ˆ¼•É¥6| \²…
E¯D¦ôM=ó7”‡¿;¬u›› áfŠFoQ2±œùË‘˜ˆ[±"¶5$7îw¹À¯è ‘ŠµÚÕ\¬\<kßJ…ÒD,
#=íŠeŒƒ×¦|€šµ(;‚qò=&±ˆ
TÝdp‘Á#²›!”{ÏÁµ¯—›˜Ö/PEÕTaVÛ¦‚‚C»ú
é´#,aßd, tëÒ´p®HƒÂZæ–]ûÂ’ŒŸ‚Ú"I²I ê9Ø?S,ôÈP åUAªÓ±1ù€
VGLã±ƒˆ.· CŽ?r°Y:îI„VáÒø¤pŽçµ&×Up´VCi ª=ÇÈ¿w«‰RÒ°ÿŒ08
,"˜<åÌNÍ¯)|Žä&irÑÚ»€H‘À¾ë(¶[T 0.žÌ‡Q~†˜Åçö ¾.½mº¦&Îì.±j 9Ñû‹ˆŽ
(ÊÔ~ÛbÈäNÆ‚¹%Ý} ³øc–÷¥¢! £äÚneÛ?)W6¿gjÎÔŽnödhl>ÿ#–
f"*,SŠU,"ÏÍtÔD”m 'ÇFƒÓ &IÝ%‰µ#3¡bÚ@Þe6öÆ}?›ëGpS– mŸ€Ï¢>µò‘ÃÏÛ–7ÅŸ…?°>
‰Ån¬jåoEr˜ÎóœÆ°•å
†DòüâÅ+O±â}A’Û&Óðä HáÑAë¤Dh>•ž×%ÖsSØžÛhëï¦ªõùË5ƒ‰SZ¤½+HZò

Ln 1, Col 1 100% Unix (LF) ANSI

3.2- FONCTIONNEMENT DU CHIFFREMENT ASYMÉTRIQUE

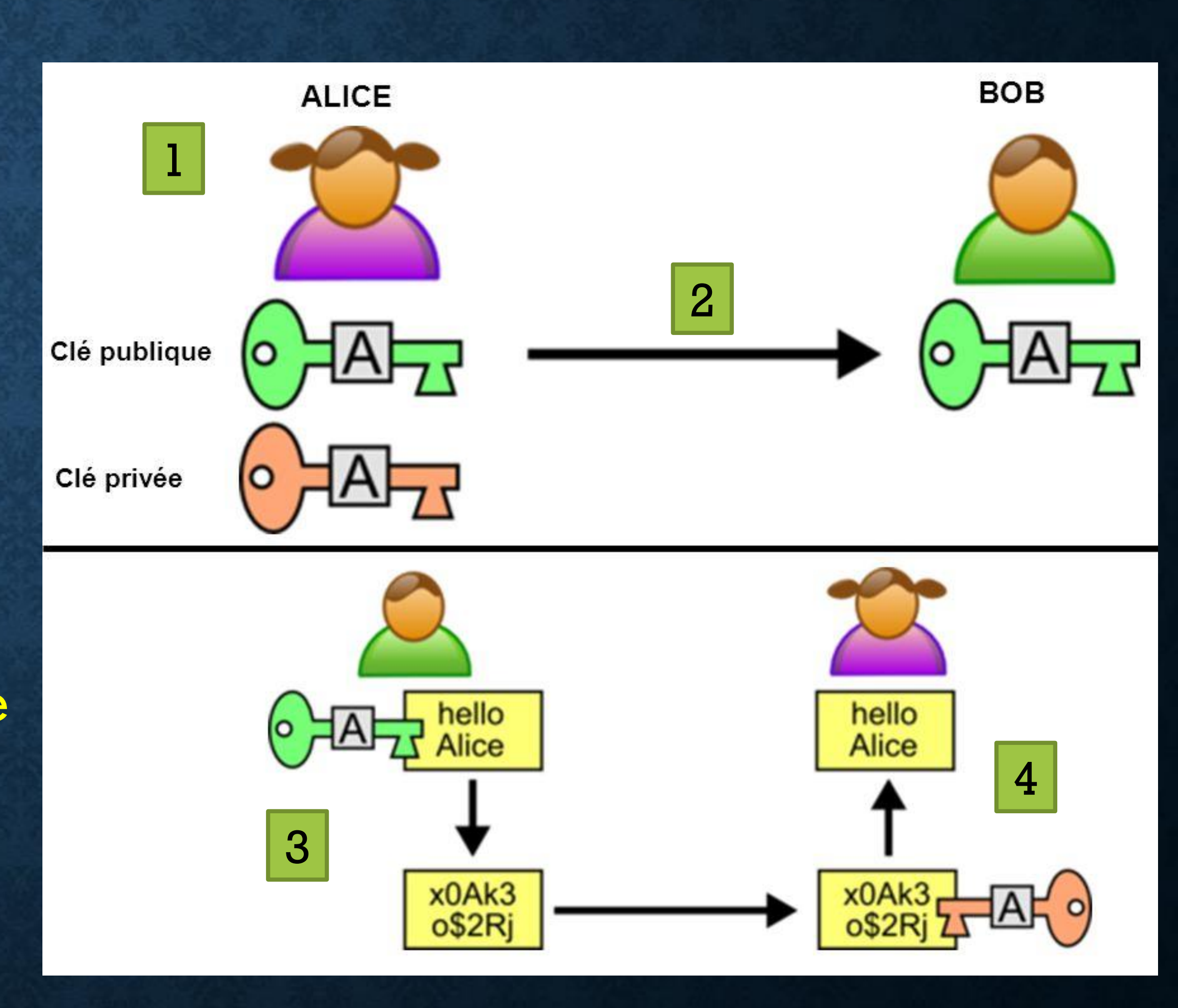
- Le deuxième type de chiffrement est le **chiffrement asymétrique** qui se repose sur l'utilisation **d'une paire de clés** et les **algorithmes de chiffrement et hachage.**
- La paire des clés (**publique** et **privée**) sont créées par l'algorithme **RSA**.
- La taille des clés peut varier entre **128 bits** à **4096 bits** et sont affiché en caractères.
- Exemple d'une clé :



3.2.1- CHIFFRER LE MESSAGE À ENVOYER

Supposons que Bob souhaite envoyer un message secret à Alice, voici comment ils doivent procéder:

1. Alice utilise le chiffrement asymétrique et génère, en utilisant un logiciel de cryptage, une clé publique et une clé privée.
   - La clé publique sert à chiffrer les messages.
   - La clé privée sert à déchiffrer les messages chiffrés.
2. Alice envoie sa clé publique à Bob.
3. Bob chiffre son message en utilisant l'algorithme de cryptage **AES** qui utilise la clé publique de Alice, puis envoie le message chiffré à Alice.
4. Alice utilise sa clé privée pour déchiffrer le message de Bob et le tour est joué.



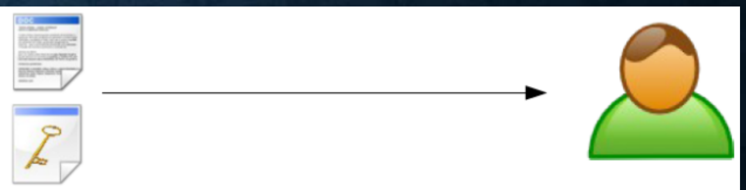
3.2.2- SIGNER LE MESSAGE À ENVOYER

Imaginons que Alice souhaite envoyer un document signé à Bob:

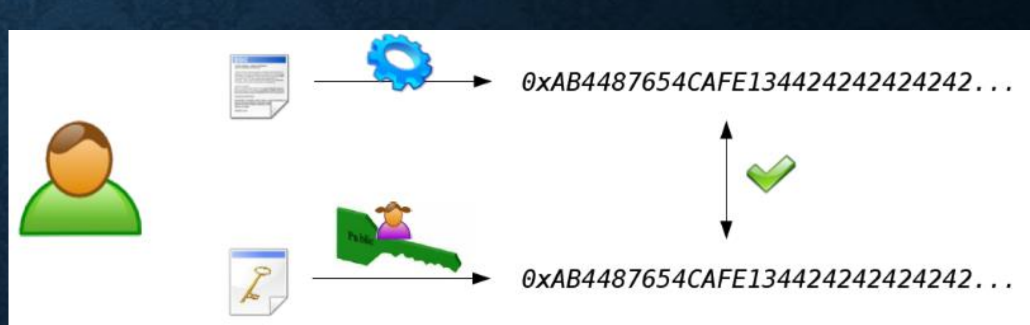
- Elle génère **la signature** du document au moyen d'un **algorithme de hachage (comme SHA-256).**
- Puis, elle **crypte** cette signature avec **sa clé privée**.

0xAB4487654CAFE134424242424242...

- Elle envoie le document avec sa signature à Bob.



- Pour vérifier la validité du document, Bob doit **déchiffrer la signature** en utilisant **la clé publique d'Alice**.
- Si cela ne fonctionne pas, c'est que le document n'a pas été envoyé par Alice.
- Si la signature est validée, donc c'est Alice qui a envoyé le document.



3.2- FONCTIONNEMENT DU CHIFFREMENT ASYMÉTRIQUE

1. **Chiffrer le message à envoyer :**
   - L'expéditeur utilise la **clé publique** du destinataire pour chiffrer son message.
   - Le destinataire utilise sa **clé privée** pour déchiffrer le message de l'expéditeur, garantissant la **confidentialité du contenu.**
   - L'**algorithme de chiffrement** asymétrique le plus connu est **AES** (Advanced Encryption Standard).

2. **S'assurer de l'authenticité de l'expéditeur :**
   - L'expéditeur utilise sa **clé privée** pour signer un message que le destinataire peut déchiffrer avec la **clé publique** de l'expéditeur, c'est le mécanisme utilisé pour **authentifier l'auteur d'un message.**
   - Cette méthode utilise un **algorithme de hachage** comme **SHA-256** qui est le plus utilisé.

4- ATTAQUE DE L'HOMME DU MILIEU (MAN-IN-THE-MIDDLE)

- L'attaque de **l'homme du milieu (Man-in-the-middle attack),** est une attaque qui a pour but d'intercepter les communications entre deux parties.

- Mais, si la communication était chiffré et tant que l'homme du milieu ne possède pas la clé privée, il ne pourra pas déchiffrer le message.

- Il est donc important de bien stockée sa clé privée, qui si elle est récupérée par un tiers est alors compromise.

Avoiding **Man-in-the-Middle** Attacks

5- LOGICIELS DE CHIFFREMENT (CRYPTAGE)

- Vous allez maintenant préparer votre ordinateur au chiffrement : Il s'agit de télécharger et installer des outils nécessaires au chiffrement de vos données personnelles que nous allons apprendre à utiliser.
- Voici quelques outils:
  - Un logiciel multiplateforme (Windows, Mac et Linux) qui permet de chiffrer des disques et clé USB : VeraCrypt.



  - Des logiciels qui permettent de chiffrer des fichiers individuellement : Axcrypt (Windows), MEO (Windows/Mac).

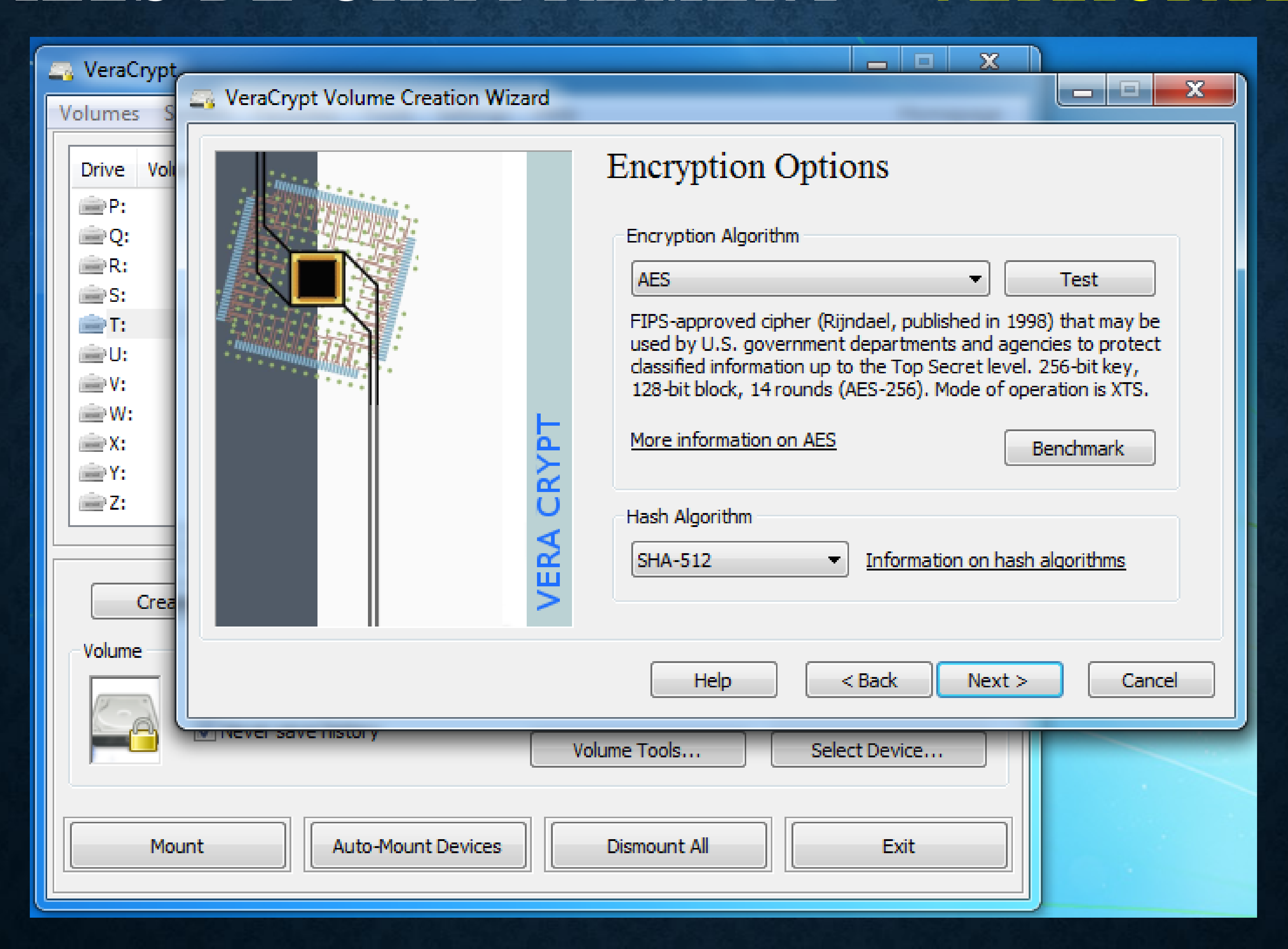




5.1- LOGICIELS DE CHIFFREMENT (CRYPTAGE) – VERACRYPT

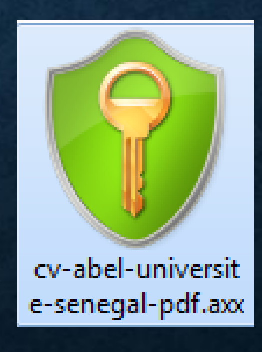
- VeraCrypt est logiciel multi-plateforme (Windows, Mac et Linux) qui permet de chiffrer des disques. Il est même possible de chiffrer une clé USB.
- L'avantage avec VeraCrypt est que les données écrites dans ces disques sont automatiquement chiffrées et déchiffrées. Pas besoin de passer son temps à chiffrer et déchiffrer manuellement des fichiers pour travailler : c'est transparent.
- En plus, c'est un outil libre et gratuit.
- Téléchargement et installation:
  - Rendez-vous sur: https://www.veracrypt.fr/en/Downloads.html et cliquez sur le lien correspondant à votre système d'exploitation (OS) pour démarrer le téléchargement.
  - Allez au dossier **Téléchargements** de votre ordinateur une fois le téléchargement fini. Procédez à l'installation comme vous le feriez avec n'importe quel logiciel.

LOGICIELS DE CHIFFREMENT - VERACRYPT



5.2- LOGICIELS DE CHIFFREMENT (CRYPTAGE) – AXCRYPT (WINDOWS)

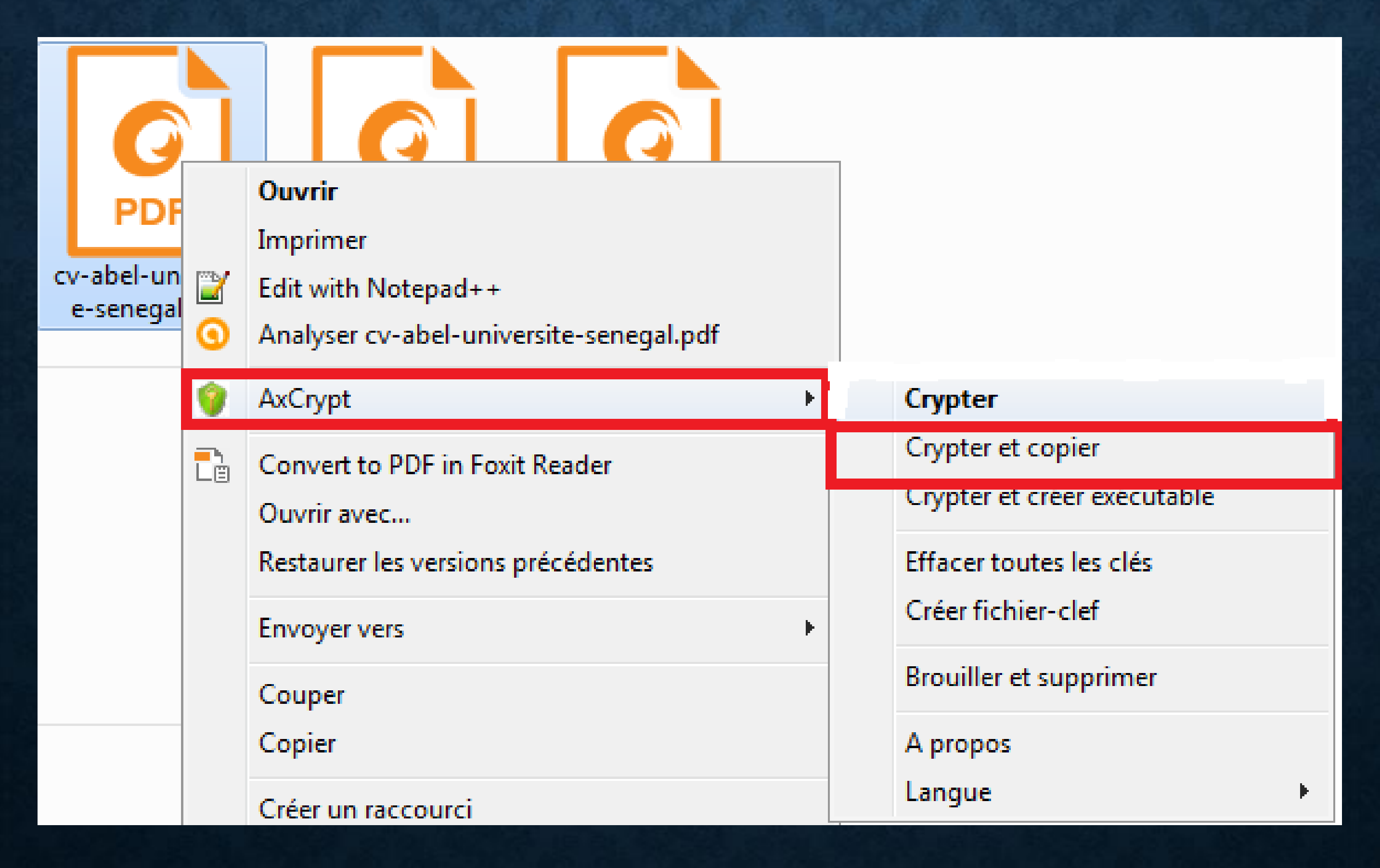
- AxCrypt est un logiciel de chiffrement permettant de protéger par mot de passe des fichiers ou des dossiers sous Windows.
- Il a l'avantage d'être intégré au menu contextuel de Windows et d'envoyer des fichiers protégés à des destinataires par mail.
- Téléchargement et installation:
  - Rendez-vous sur: **https://www.axcrypt.net/download/**
  - Après le téléchargement, démarrez l'installation en faisant un double-clic sur le fichier téléchargé et laissez-vous guider par l'installeur.
  - Exemple de fichier chiffré avec Axcrypt:



LOGICIELS DE CHIFFREMENT - AXCRYPT

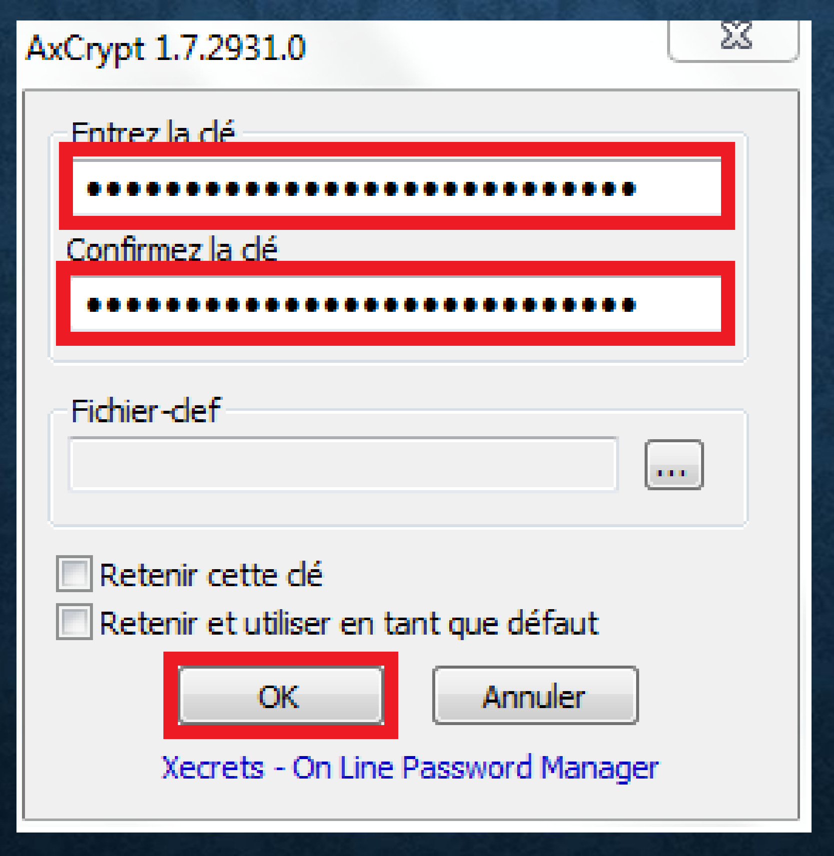
Chiffrement/déchiffrement de fichier ou dossier:

- AxCrypt offre un avantage en ce sens qu'il est intégré au clic droit de Windows. Pour chiffrer votre fichier ou dossier, faites un clic droit sur le fichier ou dossier en question, puis sélectionnez : AxCrypt > Crypter et copier.



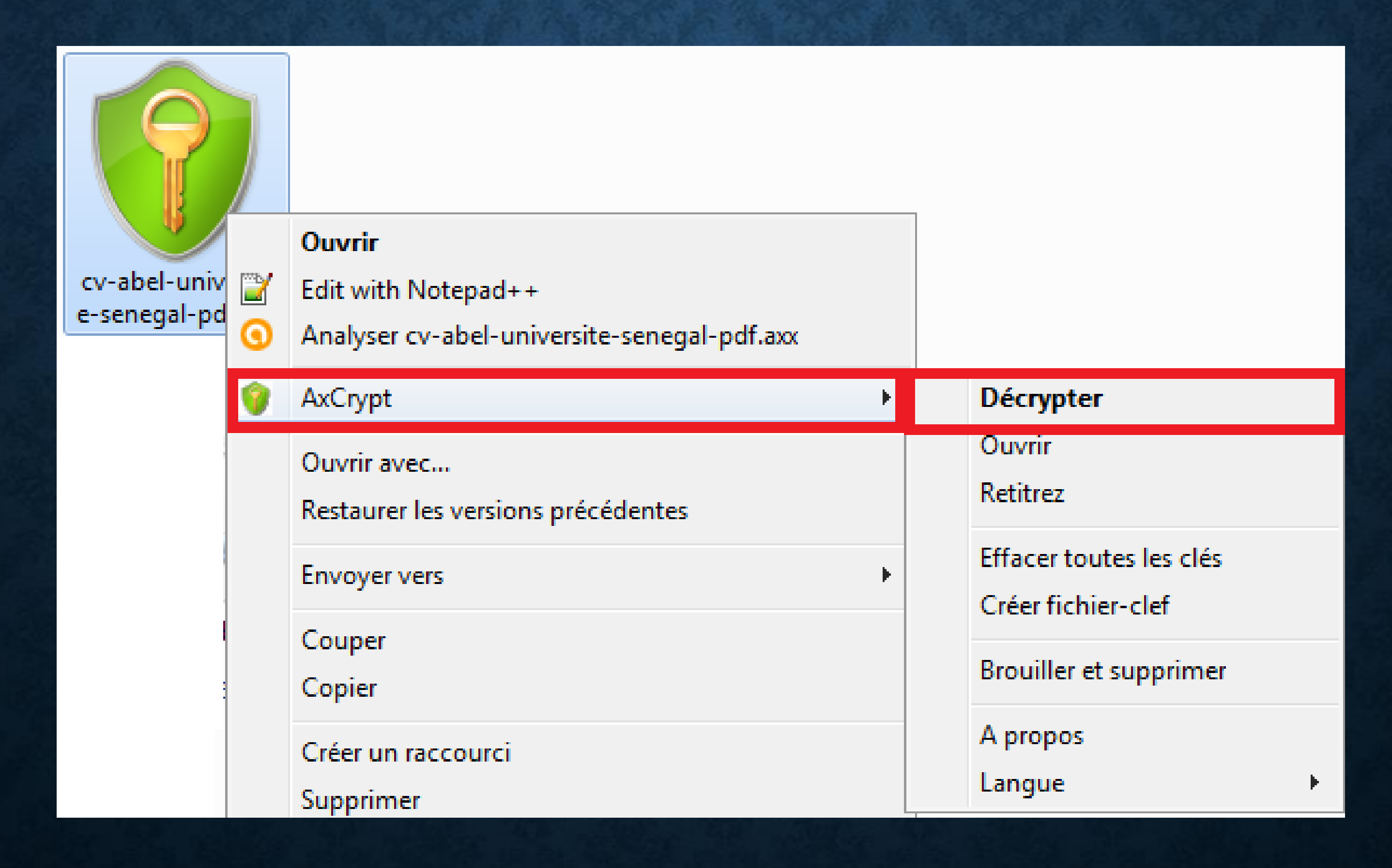
LOGICIELS DE CHIFFREMENT - AXCRYPT

- Tapez un mot de passe fort pour ce fichier (ou dossier), retapez le même mot de passe dans la zone suivante. Cliquez sur **OK.** Placez le fichier crypté dans un emplacement autre que le fichier original.



LOGICIELS DE CHIFFREMENT - AXCRYPT

- Pour **ouvrir le fichier chiffré** avec AxCrypt, double-cliquez dessus puis saisissez le mot de passe qui a servi au chiffrement.
- Pour **déchiffrer le fichier**, faites un clic droit dessus allez sur AxCrypt puis sur **Décrypter**. Entrez le mot de passe qui a servi au chiffrement.



5.3- LOGICIELS DE CHIFFREMENT (CRYPTAGE) – MEO (WINDOWS ET MAC)

- MEO est un utilitaire de chiffrement de fichiers, de dossiers et de mail, disponible sur Windows et sur Mac OS X.

- Il est gratuit pour un usage non commercial.

- Téléchargement et installation (sur MAC OS):

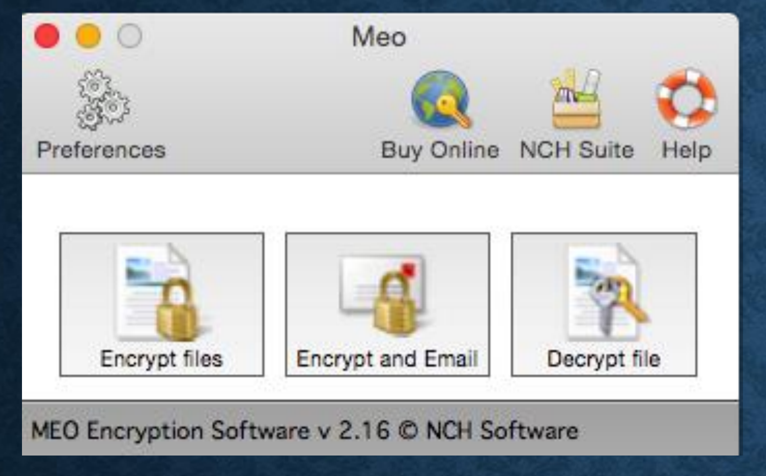
  - Rendez-vous sur: https://www.nchsoftware.com/encrypt/index.html

  - Après le téléchargement, démarrez l'installation.



LOGICIELS DE CHIFFREMENT - MEO

- Sur un ordinateur MAC, ouvrez MEO, Cliquez sur **Encrypt files**.



- Dans l'écran suivant, vous avez deux options, cliquez sur :
  - **Add File(s)**… pour ajouter un ou des fichiers.
  - **Add Folder(s)**… pour ajouter un (des) dossiers.
- Cliquez sur **Next**
- Définissez le mot de passe puis terminez en cliquant sur **Finish.**

